

A decorative graphic on the left side of the slide consisting of two overlapping parallelograms. The front one is blue and the back one is a light green color. They are positioned diagonally, with the blue one partially covering the green one.

Offensive Security and exploitation

Marian Bret

Methodology



1. Footprinting
 - scanning network scope for hosts & open ports
2. Network scanning
 - built in Kali software (nmap, dirb)
 - built in scripts (nmap-script-engine, Metasploit scanners)
 - search for possible vulnerabilities
3. Enumeration
 - searchsploit, exploit-db, CVE-details and built-in enumeration scripts
4. Exploitation
 - getting impacting information or vertical/horizontal privilege escalation

Project scope

- The project scope is 10.10.10.0/24
- The first machine of the scope is : 10.10.10.1
- The last machine of the scope is : 10.10.10.254



UDP	194.78.180	ESTABLISHED	6033	CORP
TCP	74.64.125.135	CLOSE_WAIT	80	OTHER
TCP	114.45.20.46	ESTABLISHED	12001	CORP
TCP	65.54.167.16	CLOSE_WAIT	39247	PROD
UDP	111.227.77.174	CLOSE_WAIT	443	CORP
TCP	192.168.0.44	ESTABLISHED	4029	CORP
TCP	124.40.223.226	ESTABLISHED	2916	OTHER
TCP	51.110	ESTABLISHED	12350	CEDC

© CanStockPhoto.com



10.10.10.22:139:445

- open ports 139 and 445 (SMB)
- found SMB versions v1, v2, v3
- found users 'myles' and 'guest'
- access to Public shared folder
- password protected zip file
- JohnTheRipper cracked the zip file, and file returned the password for user 'myles'
- *privilege escalation to 'myles' smb profile*



Advice:

protect the Public directory and/or the data accessible on the smb server

10.10.10.53:21



- open port 21 (FTP)
- connected to ftp service as an anonymous user
- read privilege
- ftp version vsftpd 2.3.4 vulnerable with a backdoor (CVE-73573) from searchsploit
- *privilege escalation to root shell*
- JohnTheRipper cracked the `/etc/passwd` and `/etc/shadow` files
- found credential `fern11:naruto1`
- connected to ftp service as user 'fern11'
- found ssh configuration and ssh keys

Advice:

update the ftp service from vsftpd 2.3.4 to the newest version



10.10.10.53:22

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAuvc...> ssh
```

- open port 80 (SSH)
- found version OpenSSH7.2
- connected with credential *fern11:naruto1* from 10.10.10.53:21 (previous slide)
- dumped both the private and public ssh key

Advice:

use key pairs connection instead of simple password connection
update the ftp service from vsftpd 2.3.4 to the newest version



10.10.10.222:80



WORDPRESS

- open port 80 (HTTP with Wordpress)
- found robots.txt file
- found user 'Fraser'
- found Wordpress plugin 'Akismet'
 - Akismet has multiple cross-site-scripting vulnerabilities (searchsploit)
- found XMLRPC.php
 - POST request exploits reveals huge security flaws
 - using 'system.listMethods' returned all available methods
 - found several methods 'wp.getUsersBlogs', 'wp.getCategories', 'metaWeblog.getUsersBlogs' vulnerable to login bruteforcing
 - no connection attempts limit

Advice:

replace XMLRPC protocol with REST API

update Akismet plugin's version

10.10.10.10:53 and 10.10.10.11:53

- open port 53 (TCP/UDP port with DNS service)
- found DNS service version: dnsmasq-2.75
- nslookup tool
 - linked domain name was *'dns1.powerzio.lan'* and *'dns2.powerzio.lan'*
- dig tool
 - returned the 'RA' flag that stands for 'Recursion available'
 - recursive DNS can be used to launch Ddos or cache poisoning attacks
- dnsrecon tool
 - found 17 and 12 PTR records on the range with useful information





10.10.10.11:53

- open port 53 (TCP/UDP port with DNS service)
- found DNS service version: dnsmasq-2.75
- nslookup tool
 - linked domain name was *'dns2.powerzio.lan'*
- dig tool
 - returned the 'RA' flag that stands for 'Recursion available'
 - recursive DNS can be used to launch Ddos or cache poisoning attacks
- dnsrecon tool
 - found 17 PTR records on the range with useful information



10.10.10.48:80 and 10.10.10.55:80



- open port 80 (HTTP, nodeJS with Express)
- http-cors allows *HEAD GET POST PUT DELETE PATCH* http methods on the server
- scanning with tool ZAP from OWASP society
- 1 high risk alert, 3 medium risk alerts, 3 low risk alerts
- highest risk vulnerability:
 - remote OS command injection through /api/config
 - `<script type="text/javascript">window.location="/";</script>`
 - server accepts untrusted input and data through this endpoint

Advice:

use library calls instead of external calls

make sure that important data can't be accessed with unauthenticated endpoints



10.10.10.55:80



Express.js




- open port 80 (HTTP, nodeJS with Express)
- http-cors allows *HEAD GET POST PUT DELETE PATCH* http methods on the server
- scanning with tool ZAP from OWASP society
- 1 high risk alert, 3 medium risk alerts, 3 low risk alerts
- highest risk vulnerability:
 - remote OS command injection through /api/config
 - `<script type="text/javascript">window.location="/";</script>`
 - server accepts untrusted input and data through this endpoint

Advice:

use library calls instead of external calls

make sure that important data can't be accessed with unauthenticated endpoints



The End

Thank you for watching :)

Have a nice day!